IN THE CLAIMS:

1. (Amended) A method for electronic commerce, comprising:

forming a four party payment protocol for electronic sales including a consumer's computer coupled to a merchant's computer and to an issuing bank computer via an issuer gateway, the merchant computer being further coupled to an acquiring bank computer;

sending from a merchant's computer over an internet network to a consumer's computer, a merchant message including a wallet initiation message, a merchant digital signature, and a digital certificate from an acquiring bank, said wallet initiation message including a payment amount, an order description, and a timestamp;

starting a consumer's wallet program in said consumer's computer in response to said wallet initiation message;

sending from said consumer's computer consumer identity and authentication information and said merchant message, to an issuer gateway for an issuing bank;

the issuing bank creating a reference number or value representing the consumer's credit or debit card number by repairing a table of credit card or debit card numbers and a corresponding table of reference numbers, the issuing bank pairing the consumer's card number with a selected reference number and outputting the reference number to the issuer gateway;

verifying at said issuer gateway said merchant's signature to prove that the consumer is dealing with the actual merchant and validating at said issuer gateway the merchant's certificate and the acquirer's certificate to prove that the merchant and issuer share a common financial arrangement;

said issuer gateway verifying the consumer's account and ensuring that at least one of funds [and/or] and credit are available to support the payment amount, then authorizing payment by sending to the consumer over said internet network an authorization token, an issuer's digital certificate, said wallet initiation message, and a reference to said consumer's credit or debit card number;

said authorization token including the payment amount, order description, timestamp, a random nonce plus a merchant identifier and a reference to the consumer's credit or debit card number; and

said merchant's computer receiving said authorization token and fulfilling said order description.

2. (Original) The method for electronic commerce of claim 1, which further comprises:

sending from said consumer's computer a start message over the internet network to the merchants computer, to initiate said merchant's message.

3. (Canceled)

4. (Original) The method for electronic commerce of claim 1, wherein said merchant's computer further performs the steps comprising:

receiving said authorization token;

verifying the issuer's signature, digital certificate, the payment amount and merchant identity in the authorization token;

verifying the freshness of the authorization token via the timestamp in the token;

using the nonce in the authorization token to recognize duplicate tokens; and

fulfilling said order description.

5-14. (Canceled)

15. (Original) The method for electronic commerce of claim 1, wherein said issuer gateway sends said authorization token to said consumer, and the consumer forwards said authorization token to said merchant.

16. (Original) The method for electronic commerce of claim 1, wherein said issuer gateway sends said authorization token directly to said merchant.

17. (Original) The method for electronic commerce of claim 1, wherein said reference to said credit card is an alias card number that is mapped at the issuing bank to the real card

number, thereby preventing use of the consumer's credit card number without said authorization token.

18. (Original) The method for electronic commerce of claim 1, wherein said reference to said card is an authorization number allocated uniquely by the issuer gateway for each authorization, enabling it to be passed by an acquirer gateway back to the issuing bank in a capture message;

said issuing bank maintaining a database mapping authorization numbers to card numbers, so that when the issuing bank receives the capture message, it uses the database mapping to determine the consumer's card number.

19-23. (Canceled)

24. (Amended) The method for electronic commerce of claim 1, wherein split shipments are supported by an additional message interaction between the merchant and issuer gateway, comprising:

the merchant sending the authorization token to the issuer gateway identified in the issuer's digital certificate, including details of a split requirement, such as the amount of a first payment, the merchant authenticating the request by signing it and including the merchant's digital certificate;

the issuer gateway verifying that the merchant signing message is the same merchant that signed an original request, verifying the split request according to business and risk management policies, and responding with a new authorization token in a message to the merchant;

the merchant forwarding the new authorization token in a capture message the acquirer gateway;

the merchant resubmitting the new authorization token to the acquirer gateway [m] in a second message, whenever the merchant has shipped a second part of the shipment.

25. (Original) The method for electronic commerce of claim 1, comprising:

the issuer offering the consumer a payment schedule conditioned on the merchant name from the merchant's digital certificate and the amount of payment from the initiation message.

26. (Original) The method of claim 1 further comprising:

sending a capture request message including the reference number representing the consumer's card number over the internet from the merchant to an acquirer gateway operating on behalf of an acquirer bank to capture the transaction and disburse payment to the merchant.

27. (Original) The method of claim 1 further comprising the step of:

settling accounts with the issuing bank by the acquiring bank over a private network by sending a settlement message that includes the reference number to the consumer's card number.

28. (Original) The method of claim 1 further comprising the step of

converting the reference number into the consumer's card number by the issuing bank and applying the transaction amount to the consumer's balance in his credit card or deposit account.

29. (Original) The method of claim 1 further comprising the step of:

proving that the issuing bank authorized the payment to the merchant by the combination of the issuing bank's signature on the authorization token, digital certificate, and the contents of the authorization token, providing undeniable proof that the issuing bank authorized the payment.

30-54. (Canceled)

55. (New) A method of operating a four party payment protocol in accordance with a gateway associated with an issuing bank, the method comprising the steps of:

receiving at the gateway, from a computer of a consumer, information associated with the consumer computer and a merchant message from a computer of a merchant with which the

consumer is engaging in a transaction, the merchant message comprising a wallet initiation message comprising a payment amount, an order description, a merchant identifier and a timestamp;

receiving at the gateway, from the issuing bank, a reference number, the reference number having been created by the issuing bank and representing a credit card number or a debit card number of the consumer, the issuing bank maintaining a table of credit card numbers or debit card numbers and corresponding reference numbers wherein the consumer's card number is paired with the reference number;

verifying at the gateway an account of the consumer and ensuring that at least one of funds and credit support the payment amount; and

authorizing payment by sending an authorization token, the authorization token comprising the payment amount, the order description, the merchant identifier, the timestamp, and the reference number, wherein the merchant's computer receives the authorization token initiates fulfillment of the order description, and sends a capture request message comprising the reference number, to an acquirer bank;

wherein the acquirer bank captures the transaction and disburses payment to the merchant; and further

wherein the issuing bank, in response to a message from the acquirer bank, converts the reference number into the consumer's credit or debit card number and applies the payment amount to a balance in the account of the consumer.

56. (New) The method of claim 55, wherein the gateway associated with the issuing bank sends the authorization token to the merchant computer via the consumer computer.

57. (New) The method of claim 55, wherein the gateway associated with the issuing bank sends the authorization token directly to the merchant computer.

58. (New) The method of claim 55, further comprising the step of the gateway associated with the issuing bank signing the authorization token.

59-60. (Canceled)

61. (New) A method of operating a four party payment protocol in accordance with a computer of a merchant, the method comprising the steps of:

sending a message from the merchant computer to a computer of a consumer with which the merchant computer is engaging in a transaction, the merchant message comprising a wallet initiation message, the wallet initiation message comprising a payment amount, an order description, a merchant identifier and a timestamp, wherein the merchant message is sent to a gateway associated with an issuing bank, via the consumer computer, along with information associated with the consumer computer;

receiving at the merchant computer an authorization token sent by the gateway after the gateway has verified an account of the consumer and ensured that at least one of funds and credit support the payment amount, the authorization token comprising the payment amount, the order description, the merchant identifier, the timestamp, and a reference number, the reference number having been created by the issuing bank and representing a credit card number or a debit card number and corresponding reference numbers wherein the consumer's card number is paired with the reference number;

initiating fulfillment of the order description at the merchant computer; and

sending from the merchant computer to an acquirer bank, a capture request message comprising the reference number,

wherein the acquirer bank captures the transaction and disburses payment to the merchant; and further

wherein the issuing bank, in response to a message from the acquirer bank, converts the reference number into the consumer's credit or debit card number and applies the payment amount to a balance in the account of the consumer.

62-67. (Canceled)

68. (New) The method for electronic commerce of claim 1, wherein said wallet initiation message includes a nonce.

69. (New) The method for electronic commerce of claim 1, wherein said consumer identity and authentication information is a userid and a password.

70. (New) The method for electronic commerce of claim 1, wherein said consumer identity and authentication information is an ATM debit card number and PIN.

71. (New) The method for electronic commerce of claim 1, wherein said consumer identity and authentication information is a smart card's account number and a symmetric Message Authentication Code (MAC).

72. (New) The method for electronic commerce of claim 1, wherein said consumer identity and authentication information is a smart card's account number and an asymmetric digital signature.

73. (New) The method for electronic commerce of claim 1, wherein said consumer identity and authentication information is a consumer's digital signature and digital certificate.

74. (New) The method for electronic commerce of claim 1, wherein said authorization token includes a dummy card number for use in routing payment to an appropriate one of a plurality of issuing banks;

said dummy card number being shared among all cardholders of a particular issuing bank.

75. (New) The method for electronic commerce of claim 1, wherein said consumer identity and authentication information is a consumer's digital certificate and matching asymmetric digital signature.

76. (New) The method for electronic commerce of claim 1, wherein said consumer identity and authentication information is a user account number and a symmetric MAC or asymmetric digital signature.

77. (New) The method for electronic commerce of claim 1, wherein said consumer identity and authentication information is a user account number and an asymmetric digital signature.

78. (New) The method for electronic commerce of claim 1, wherein said consumer identity information is a consumer's biometric signal.

79. (New) The method for electronic commerce of claim 1, which further comprises:
a digital certificate hierarchy that covers issuing banks, acquiring banks, and merchants.

80. (New) The method for electronic commerce of claim 79, wherein said certificate hierarchy is used with public-key digital signatures to identify said merchant and said issuing bank.

81. (New) The method for electronic commerce of claim 80, wherein said certificates represent common financial agreements and obligations among said merchant and said issuing bank.

82. (New) The method for electronic commerce of claim 81, wherein the issuing bank certificates identify and help authenticate issuing banks to merchants, providing a basis for the merchants to trust the authorization tokens provided by the issuing banks.

83. (New) The method for electronic commerce of claim 82, wherein an acquiring bank certificate and a merchant certificate identify and help authenticate said acquiring bank and said

merchant to issuing banks;

said merchant certificate identifying the merchant to the consumer and verifying that the merchant is a valid participant of a payment scheme, before the issuing bank provides said authorization token.

84. (New) A method of providing at least a part of a four party payment service, the part of the service being provided in accordance with a gateway associated with an issuing bank, the method comprising the steps of:

receiving at the gateway, from a computer of a consumer, information associated with the consumer computer and a merchant message from a computer of a merchant with which the consumer is engaging in a transaction, the merchant message comprising a wallet initiation message comprising a payment amount, an order description, a merchant identifier and a timestamp;

receiving at the gateway, from the issuing bank, a reference number, the reference number having been created by the issuing bank and representing a credit card number or a debit card number of the consumer, the issuing bank maintaining a table of credit card numbers or debit card numbers and corresponding reference numbers wherein the consumer's card number is paired with the reference number;

verifying at the gateway an account of the consumer and ensuring that at least one of funds and credit support the payment amount; and

authorizing payment by sending an authorization token, the authorization token comprising the payment amount, the order description, the merchant identifier, the timestamp, and the reference number, wherein the merchant's computer receives the authorization token initiates fulfillment of the order description, and sends a capture request message comprising the reference number, to an acquirer bank;

wherein the acquirer bank captures the transaction and disburses payment to the merchant; and further

wherein the issuing bank, in response to a message from the acquirer bank, converts the reference number into the consumer's credit or debit card number and applies the payment

amount to a balance in the account of the consumer.

85. (New) The method of claim 84, wherein the gateway associated with the issuing bank sends the authorization token to the merchant computer via the consumer computer.

86. (New) The method of claim 84, wherein the gateway associated with the issuing bank sends the authorization token directly to the merchant computer.

87. (New) The method of claim 84, further comprising the step of the gateway associated with the issuing bank signing the authorization token.

88. (New) A method of providing at least a part of a four party payment service, the part of the service being provided in accordance with a computer of a merchant, the method comprising the steps of:

sending a message from the merchant computer to a computer of a consumer with which the merchant computer is engaging in a transaction, the merchant message comprising a wallet initiation message, the wallet initiation message comprising a payment amount, an order description, a merchant identifier and a timestamp, wherein the merchant message is sent to a gateway associated with an issuing bank, via the consumer computer, along with information associated with the consumer computer;

receiving at the merchant computer an authorization token sent by the gateway after the gateway has verified an account of the consumer and ensured that at least one of funds and credit support the payment amount, the authorization token comprising the payment amount, the order description, the merchant identifier, the timestamp, and a reference number, the reference number having been created by the issuing bank and representing a credit card number or a debit card number and corresponding reference numbers wherein the consumer's card number is paired with the reference number;

initiating fulfillment of the order description at the merchant computer; and

sending from the merchant computer to an acquirer bank, a capture request message

comprising the reference number,

wherein the acquirer bank captures the transaction and disburses payment to the merchant; and further

wherein the issuing bank, in response to a message from the acquirer bank, converts the reference number into the consumer's credit or debit card number and applies the payment amount to a balance in the account of the consumer.

89. (New) A method of operating a four party payment protocol in accordance with a gateway associated with an issuing bank, the method comprising the steps of:

receiving at the gateway, from a computer of a consumer, information associated with the consumer computer and a merchant message from a computer of a merchant with which the consumer is engaging in a transaction, the merchant message comprising a wallet initiation message comprising a payment amount, an order description, a merchant identifier and a timestamp;

receiving at the gateway, from the issuing bank, a reference number, the reference number having been created by the issuing bank and representing a credit card number or a debit card number of the consumer, the issuing bank maintaining a mapping of credit card numbers or debit card numbers and corresponding reference numbers wherein the consumer's card number is paired with the reference number;

verifying at the gateway an account of the consumer and ensuring that at least one of funds and credit support the payment amount; and

authorizing payment by sending an authorization token, the authorization token comprising the payment amount, the order description, the merchant identifier, the timestamp, and the reference number, wherein the merchant's computer receives the authorization token initiates fulfillment of the order description, and sends a capture request message comprising the reference number, to an acquirer bank;

wherein the acquirer bank captures the transaction and disburses payment to the merchant; and further

wherein the issuing bank, in response to a message from the acquirer bank, converts the

reference number into the consumer's credit or debit card number and applies the payment amount to a balance in the account of the consumer.

90. (New) The method of claim 89, wherein the gateway associated with the issuing bank sends the authorization token to the merchant computer via the consumer computer.

91. (New) The method of claim 89, wherein the gateway associated with the issuing bank sends the authorization token directly to the merchant computer.

92. (New) The method of claim 89, further comprising the step of the gateway associated with the issuing bank signing the authorization token.

93. (New) A method of operating a four party payment protocol in accordance with a computer of a merchant, the method comprising the steps of:

sending a message from the merchant computer to a computer of a consumer with which the merchant computer is engaging in a transaction, the merchant message comprising a wallet initiation message, the wallet initiation message comprising a payment amount, an order description, a merchant identifier and a timestamp, wherein the merchant message is sent to a gateway associated with an issuing bank, via the consumer computer, along with information associated with the consumer computer;

receiving at the merchant computer an authorization token sent by the gateway after the gateway has verified an account of the consumer and ensured that at least one of funds and credit support the payment amount, the authorization token comprising the payment amount, the order description, the merchant identifier, the timestamp, and a reference number, the reference number having been created by the issuing bank and representing a credit card number or a debit card number and corresponding reference numbers wherein the consumer's card number is paired with the reference number;

initiating fulfillment of the order description at the merchant computer; and

sending from the merchant computer to an acquirer bank, a capture request message

comprising the reference number,

wherein the acquirer bank captures the transaction and disburses payment to the merchant; and further

wherein the issuing bank, in response to a message from the acquirer bank, converts the reference number into the consumer's credit or debit card number and applies the payment amount to a balance in the account of the consumer.